(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 April 2001 (19.04.2001)

PCT

(10) International Publication Number
WO 01/28273 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/FI00/00873

(22) International Filing Date: 11 October 2000 (11.10.2000)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
19992185 11 October 1999 (11.10.1999) FI

(71) Applicant *(for all designated States except US)*: **SONERA OYJ** [FI/FI]; Teollisuuskatu 15, FIN-00510 Helsinki (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LAMMI, Tapio** [FI/FI]; Korpimaankatu 7 D, FIN-53850 Lappeenranta (FI). **LINDQVIST, Anssi** [FI/FI]; Sofianlehdonkatu 11 B 12, FIN-00610 Helsinki (FI). **RUOTTINEN, Timo** [FI/FI]; Korpraalinkuja 3 As 301, FIN-53810 Lappeenranta (FI).

(74) Agent: **PAPULA OY**; P.O. Box 981, FIN-00101 Helsinki (FI).

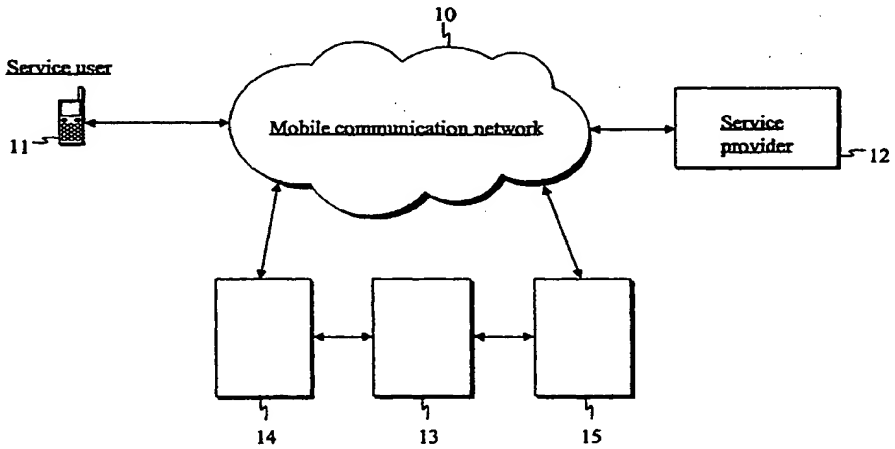
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A METHOD AND SYSTEM FOR PROTECTING A USER IDENTIFIER



(57) Abstract: The present invention relates to a method and a system for protecting the user identifier of a service user from the service provider in a mobile communication network, which service to be provided/used is a content service utilizing the geographical information of the service user. The system comprises a terminal device of the service user (11) for sending the service request to the service provider; equipment of the service provider (12) for generating the service response and sending it to the service user; and a mobile communication network (10) for transmitting the service request and the service response. In accordance with the invention, the system comprises an encrypting device (13) for generating the service-request-specific anonymous identifier corresponding to the user identifier; an identification database (13) for storing the user identifier and corresponding anonymous identifier; a service gateway (14) for retrieving the user identifier and the anonymous identifier corresponding to one another and for substituting the identifiers in question with one another in the service requests and service responses directed to the service gateway in question; and a location register (15) for retrieving the user identifier corresponding to the anonymous identifier as well as for retrieving the geographical information of the service user based on the user identifier in question.

WO 01/28273 A1

A METHOD AND SYSTEM FOR PROTECTING A USER IDENTIFIER

FIELD OF THE INVENTION

The invention relates to telecommunication systems. More specifically, the invention relates to a method and a system for protecting the user identifier of a service user from the service provider in a mobile communication network, which service concerned is a content service utilizing the geographical information of the service user.

PRIOR ART

The network operators of the mobile communication networks have remarkably increased the number of their services and the co-operation with the service providers in the last few years. The number of services is wide, and most of the services do not require any specific solutions of the operator, e.g. for guaranteeing the protection of identity of the user. Nowadays, the operators are, however, willing to develop, e.g. their content services, and the meaning of the protection of identity is remarkably emphasized, because the services provided may include sensitive information comparable, e.g. with the geographical information. Generally, people speak about a client, which means the user of the service, and about a network operator or a telephone operator who offer network services, such as call transfer, call waiting, answering services, conference calls, etc. Now as a third party, there are the content providers who are hereinafter referred to as service providers. These interest groups provide content services, such as horoscopes, news services, timetables etc. The appearing of a third party in between the client and the network operator may cause changes to the compiling of such identifiers that may insult the protection of data privacy of the client, i.e. the user of the serv-

ice. According to the present legislation, the content provider cannot be given such information that might insult the protection of identity of the client.

For example in the GSM, there are several registers defined that are different databases. On the home location register HLR, there are the subscriber details permanently stored that are needed in the production of services regardless of the fact of where the subscriber each time is located. Such subscriber details are, e.g. the international mobile subscriber identity (IMSI, International Mobile Subscriber Identity), the mobile station ISDN number (MSISDN), additional services agreed by the subscriber, certain information of the location of that moment of the subscriber. Prior-art technique represents also the servicing mobile location centre (SMLC, Servicing Mobile Location Centre), which is used in locating the position of that time of the user of the service. Before, people used to talk about a mobile location centre (MLC, Mobile Location Centre), but now that the position of that moment of the subscriber of the services has to be accurately located, people have changed to the use of this aforementioned SMLC.

On the visitor location register VLR, the subscriber details that are needed in production of the services are stored temporarily for the period the subscriber is located in the service area of the servicing mobile location centres of the VLR. When the mobile station is detected in the service area in question, the VLR asks the HLR for these details. In addition to the information in the HLR, the temporary mobile subscriber identity (TMSI, Temporary Mobile Subscriber Identity) is stored on the VLR. This is used in signaling in radio path instead of the IMSI because the permanent identity is wished to keep secret. In addition, in the VLR there is the location area iden-

tity (LAI, Location Area Identity) of that time of the subscriber.

The authentication centre (AUC, Authentication Centre) is a database which includes subscriber details relating to the information security. The AUC checks whether the subscriber is the one who he or she claims to be (IMSI/TMSI). AUC also includes the keys of the encryption used in the radio path.

In addition, as for prior art, the meaning of the wireless application protocol (WAP, Wireless Application Protocol) is not to be ignored as an alternative way of action when planning components managing the service request of the network operator. The use of the wireless application protocol is becoming common in solutions in which a connection is needed between portable terminal devices, such as mobile stations and the Internet applications, e.g. electronic mail, WWW (World Wide Web), news groups. The wireless application protocol provides an architecture which adapts mobile phones, browser programs of mobile phones, and the WWW to work as a functional entity. A problem has become the amount of information transmitted in the network between the client, network operator and the service provider. The operator has to be able to take care of the protection of identity of the client and to try to prevent information from ending up into the hands of those not concerned. At the same time, the operator has to be able to pick up from the information flow the essential information needed in order to be able to address the service to the right subscriber.

OBJECTIVE OF THE INVENTION

The objective of the present invention is to disclose a new kind of method and system that eliminates the disadvantages referred to above, or at least significantly alleviates them. One specific objective

of the invention is to disclose a method and a system that make it possible to protect the user identifier of a service user from the service provider in a mobile communication network. However, the protection is effected at such a level that the service provider gets the information sufficient enough for him or her to be able to address the service to the right subscriber.

BRIEF DESCRIPTION OF THE INVENTION

In the present invention, a user identifier of a service user is protected from the service provider in a mobile communication network, such as the GSM network (Global System for Mobile Telecommunications, GSM). The term "service provider" refers to the provider of the content services in distinction from the telephone operator providing network services. Correspondingly, the term "service" refers to the content service in distinction from the network services. More specifically, the service is hereinafter used to refer to such a content service that utilizes the geographical information of the service user.

A service request containing the user identifier of the service user is sent from the terminal device of the service user. The user identifier means the way of identifying the user unambiguously used by the mobile station in use and known in itself, such as the MSISDN number (Mobile Subscriber Integrated Services Digital Network, MSISDN), IMEI code (International Mobile station Equipment Identity, IMEI) or the TMSI identity (Temporary Mobile Subscriber Identity, TMSI). The service request in question is transmitted to the equipment of the service provider by means of which, a service response is generated. The service response is sent from the equipment of the service

provider, and is transmitted to the terminal device of the service user.

In accordance with the invention, the service request is directed to the service gateway which asks the encrypting party for the anonymous identifier corresponding to the user identifier in question. The anonymous identifier in question is generated by means of an encryption device. The user identifier and the corresponding anonymous identifier are stored on an identification database. The anonymous identifier is sent to the service gateway in which the service request is modified in such a way that the user identifier is substituted with the anonymous identifier. After this, the modified service request is directed to the equipment of the service provider.

Further in accordance with the invention, a geographical information request containing the anonymous identifier is sent from the equipment of the service provider to the location register, which retrieves from the database a user identifier corresponding to the anonymous identifier in question. The user identifier in question helps to find out the geographical information of the service user. The geographical information and the corresponding anonymous identifier are sent to the equipment of the service provider. The service response is generated based on the geographical information in question. The service response containing the anonymous identifier is directed to the service gateway which retrieves from the identification database a user identifier corresponding to the anonymous identifier. The service response is directed to the terminal device of the service user by means of the user identifier in question.

In an embodiment of the invention, the user identifier and the corresponding anonymous identifier are eliminated from the identification database after a predetermined time.

In an embodiment of the invention, the user identifier and the corresponding anonymous identifier are eliminated from the identification database after a predetermined number of inquiries.

In an embodiment of the invention, the geographical information is found out by retrieving it from the SMLC centre (Servicing Mobile Location Centre, SMLC) of the mobile communication network.

In an embodiment of the invention, the geographical information is found out by retrieving it from the location database maintained by the location register.

In an embodiment of the invention, the service gateway is arranged in conjunction with the SMS centre (Short Message Service, SMS) of the mobile communication network.

In an embodiment of the invention, the service gateway is arranged in conjunction with the WAP gateway (Wireless Application Protocol, WAP) of the mobile communication network.

In an embodiment of the invention, the user identifier is the MSISDN number of the terminal device of the service user.

In an embodiment of the invention, the mobile communication network is a GSM network.

As compared with prior art the present invention provides the advantage that it makes it possible to protect the user identifier of the service user from the content provider. This on the other hand makes it possible to develop and/or provide such content services of a mobile communication network that utilize the geographical information of the service user because thanks to the invention, no sensitive information resulting from the combination of the identity and the location of the service user is going to end up to the third party, i.e. the content provider.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following section, the invention will be described by the aid of the attached examples of its embodiments with reference to the attached drawing, in which

Fig. 1 schematically represents one system of the invention; and

Fig. 2 schematically represents another system of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 is a flow chart illustrating one system of the invention. In the figure, the terminal device of the service user 11 has been connected to the mobile communication network 10, e.g. to a digital mobile network. From the aforementioned terminal device 11, a service request is sent to the mobile communication network 10. Connected to the aforementioned mobile communication network is also the equipment of the service provider 12, which may be, e.g. a computer or some other suitable equipment or a software configuration. The aforementioned equipment is used to maintain, e.g. the content services and address them to right clients. The system also comprises a service gateway 14 which is connected to the mobile communication network 10 and which is arranged, e.g. in conjunction with the SMS centre or the WAP gateway. Further, the service gateway may be implemented as a separate entity. In addition, the system comprises, in accordance with the invention, an encrypting device 13 in whose conjunction there is an identification database 13 arranged. In addition, the system comprises, in accordance with the invention, a location register 15 in whose conjunction it is possible to arrange a location database 15 for maintaining the geographical information.

Fig. 2 is a flow chart illustrating another method of the invention. At a step 21, from the terminal device of the service user, such as the GSM telephone, a service request containing the user identifier of the service user is sent. In the exemplary case as illustrated in the figure, the user identifier is the MSISDN number of the service user. In accordance with the invention, at a step 22, the mobile communication network directs the service request to the service gateway which at a step 23 sends to the encrypting device a request to give the anonymous identifier corresponding to the user identifier in question. The aforementioned anonymous identifier is generated by means of the encrypting device, and the user identifier and the corresponding anonymous identifier are stored on the identification database at a step 24. At a step 25, the anonymous identifier is sent to the service gateway which modifies the service request by substituting the user identifier with the anonymous identifier. After this, the modified service request is directed to the equipment of the service provider at a step 26. At a step 27, from the equipment of the service provider, a geographical information request containing the anonymous identifier is sent to the location register, which at the steps 28, 29 and 30 finds out the user identifier corresponding to the anonymous identifier in question by means of the identification database and/or the encrypting device. By means of the user identifier in question, the geographical information of the service user is found out at a step 31 using the location register. The geographical information is found out, e.g. by retrieving it from the SMLC centre (Servicing Mobile Location Centre, SMLC) of the mobile communication network. Alternatively, e.g. in the location register, a location database is maintained from which the geographical information is retrieved, if necessary. At a step 32,

the geographical information and the anonymous identifier corresponding to it are sent to the equipment of the service provider. The service response is generated based on the geographical information in question at a step 33. At a step 34, the service response containing the anonymous identifier is directed to the service gateway, which retrieves the user identifier corresponding to the anonymous identifier from the identification database by repeating the steps. The service response is directed to the terminal device of the service user based on the user identifier in question at steps 35-36.

The invention is not restricted merely to the examples of its embodiments, instead many variations are possible within the scope of the inventive idea.

CLAIMS

1. A method for protecting the user identifier of a service user from the service provider in a mobile communication network, which service to be provided/used in question is a content service utilizing the geographical information of the service user and which method comprises the steps of:

sending the service request containing the user identifier of the service user from the terminal device of the service user,

transmitting the service request in question to the equipment of the service provider,

generating the service response using the equipment of the service provider,

sending the service response from the equipment of the service provider, and

transmitting the service response to the terminal device of the service user,

characterised in that the method further comprises the steps of:

directing the service request to the service gateway,

asking the encrypting party for the service-request-specific anonymous identifier corresponding to the user identifier in question,

generating the anonymous identifier by means of the encryption device and storing the user identifier and the corresponding anonymous identifier on the identification database,

sending the anonymous identifier to the service gateway,

modifying the service request by substituting the user identifier with the anonymous identifier,

directing the modified service request to the equipment of the service provider,

sending a geographical information request containing the anonymous identifier from the equipment of the service provider to the location register,

retrieving the user identifier corresponding to the anonymous identifier in question from the identification database to the location register,

finding out the geographical information of the service user in question by means of the user identifier in question,

sending the geographical information and the corresponding anonymous identifier to the equipment of the service provider,

generating the service response based on the geographical information in question,

directing the service response containing the anonymous identifier to the service gateway,

retrieving the user identifier corresponding to the anonymous identifier from the identification database, and

directing the service response to the terminal device of the service user by means of the user identifier in question.

2. A method as defined in claim 1, characterised in that the method further comprises the step of:

eliminating the user identifier and the corresponding anonymous identifier from the identification database after a predetermined time.

3. A method as defined in claim 1, characterised in that the method further comprises the step of:

eliminating the user identifier and the corresponding anonymous identifier from the identification database after a predetermined number of inquiries.

4. A method as defined in any one of the preceding claims 1, 2, or 3, characterised in that the method further comprises the step of:

finding out the location information by retrieving it from the SMLC centre of the mobile communication network.

5. A method as defined in any one of the preceding claims 1, 2, or 3, characterised in that the method further comprises the step of:

finding out the geographical information by retrieving it from the location database maintained by the location register.

6. A system for protecting the user identifier of a service user from the service provider in a mobile communication network, which service to be provided/used is a content service utilizing the geographical information of the service user and which system comprises:

a terminal device of the service user (11) for sending the service request to the service provider, which service request comprises the user identifier of the service user,

equipment of the service provider (12) for generating the service response and sending it to the service user, and

a mobile communication network (10) for transmitting the service request and the service response,

characterised in that the system further comprises:

an encrypting device (13) for generating the service-request-specific anonymous identifier corresponding to the user identifier,

an identification database (13) for storing the user identifier and the corresponding anonymous identifier,

a service gateway (14) for retrieving the user identifier and the anonymous identifier corresponding to one another and for substituting the identifiers in question with one another in the service requests and/or service responses directed to the service gateway in question, and

a location register (15) for retrieving the user identifier corresponding to the anonymous identifier and for retrieving the geographical information of the service user based on the user identifier in question.

7. A system as defined in claim 6, characterised in that the location register (15) comprises:

means (15) for retrieving the geographical information from the SMLC centre of the mobile communication network (10).

8. A system as defined claim 6, characterised in that the location register (15) comprises:

a location database (15) for maintaining the geographical information.

9. A system as defined in any one of the preceding claims 6, 7, or 8, characterised in that the service gateway (14) has been arranged in conjunction with the SMS centre of the mobile communication network (10).

10. A system as defined in any one of the preceding claims 1, 2, or 3, characterised in that the service gateway (14) has been arranged in conjunction with the WAP gateway of the mobile communication network (10).

11. A system as defined in any one of the preceding claims 6, 7, 8, 9, or 10, characterised in that the user identifier is the MSISDN number of the terminal device of the service user (11).

12. A system as defined in any one of the preceding claims 6, 7, 8, 9, 10, or 11, characterised in that the mobile communication network (10) is a GSM network.

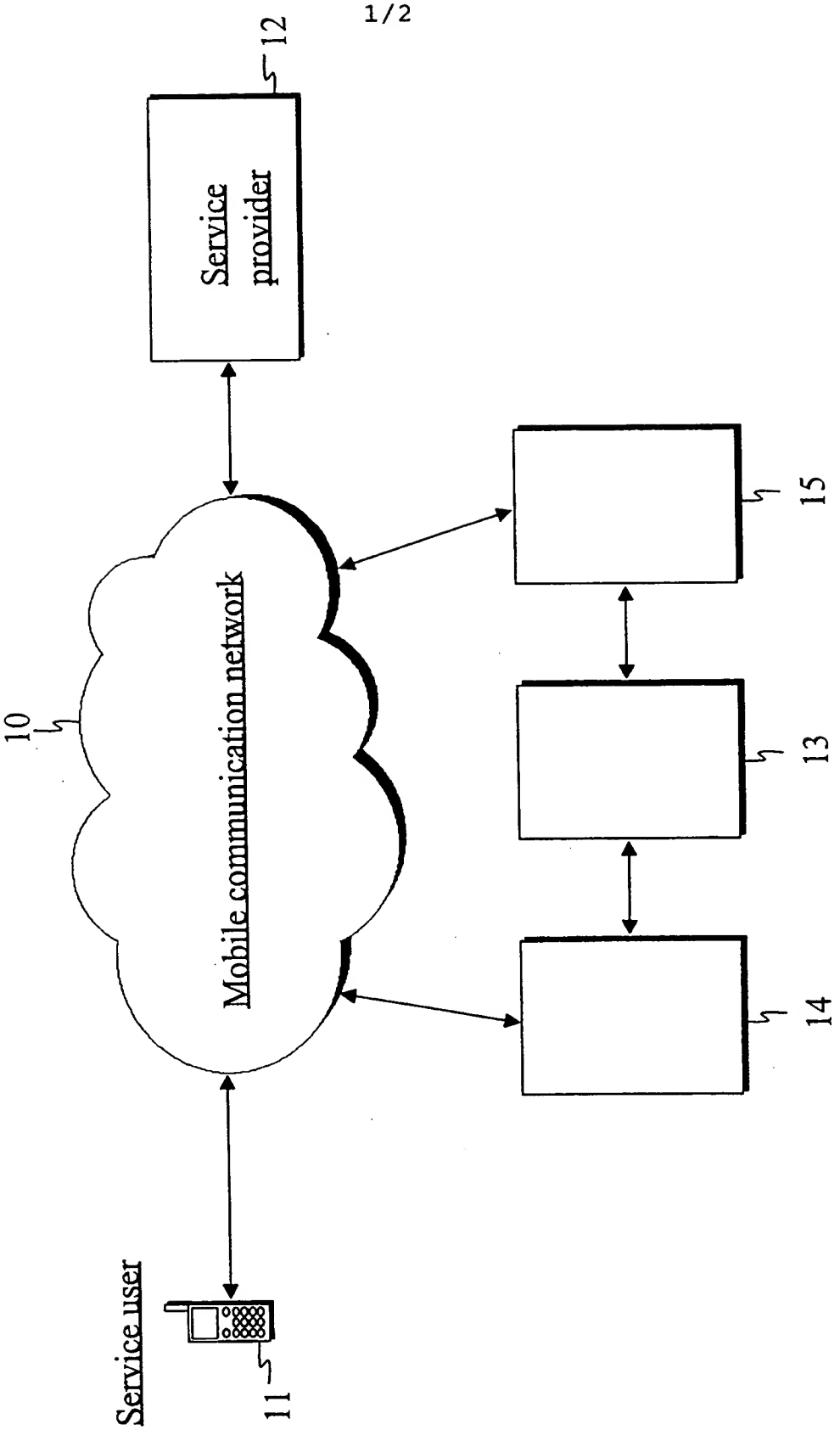

Service provider
12
Mobile communication network
10
15
13
14
Service user
11

Fig. 1

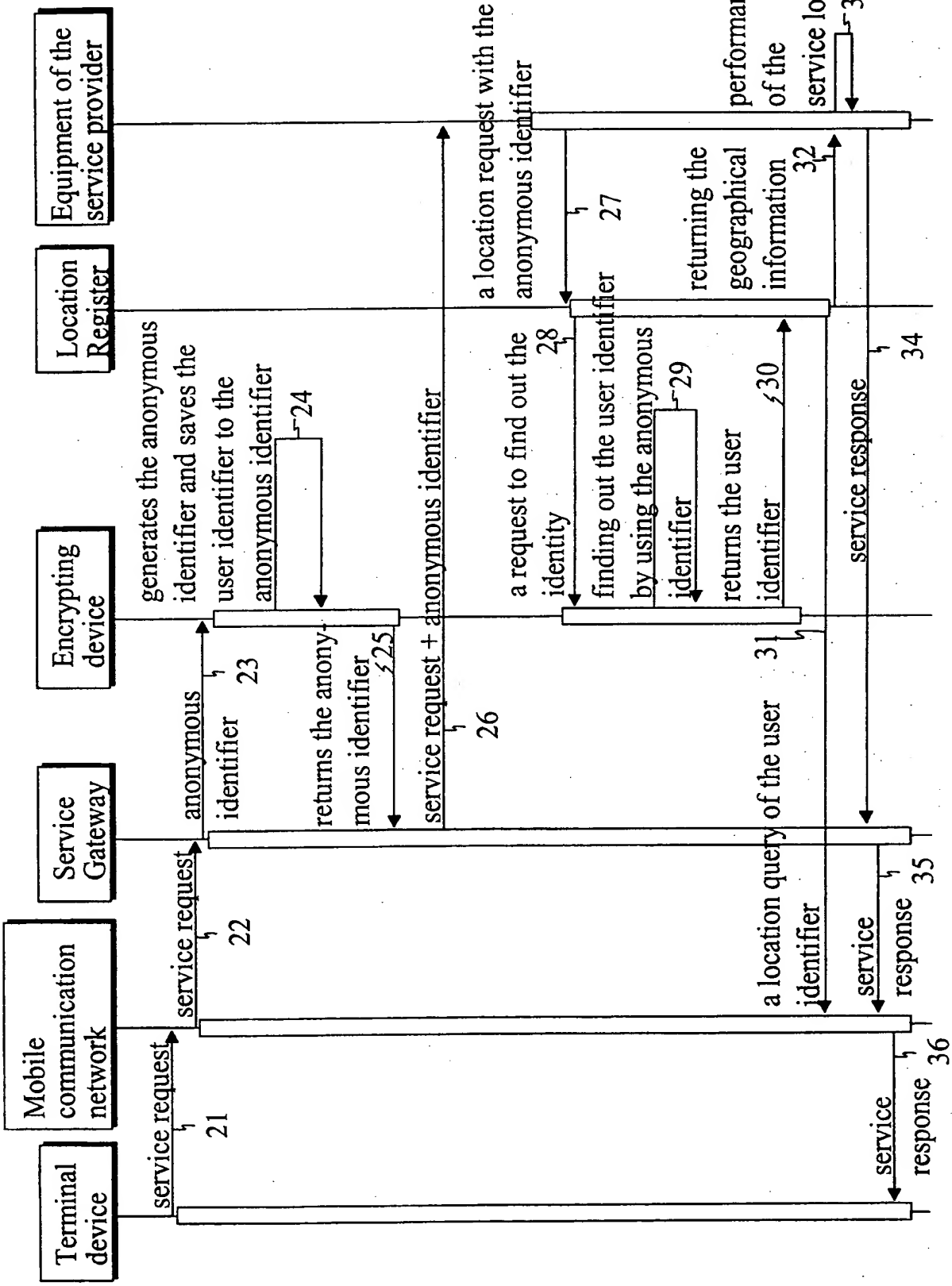


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00873

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"Achieving User Privacy in Mobile Networks" 1997-12-08 B Askwith, M Merabti, Q Shi, K Whiteley See the whole document --	1-12
P,A	EP 0982958 A2 (LUCENT TECHNOLOGIES INC.), 1 March 2000 (01.03.00), page 3, line 10 - line 30, abstract --	1-12
A	JP 10191447 A (N T T IDO TSUSHINMO KK), 21 July 1998 (21.07.98), see the whole document -- --------	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 January 2001	29 -01- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Thomas Tholin/JAn Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/12/00

International application No.
PCT/FI 00/00873

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0982958 A2	01/03/00	AU 4476099 A	16/03/00
		BR 9903783 A	05/09/00
		CN 1256596 A	14/06/00
		JP 2000115161 A	21/04/00
JP 10191447 A	21/07/98	NONE	